Golden Power

Il "potere d'oro" dei governi

"Prima di desiderare fortemente una cosa bisogna verificare quanto sia felice chi la possiede"

(F. La Rochefoucauld)

Con il decreto Legge n° 21 del 15 marzo 2012, il Governo Italiano ha voluto riscrivere, in modo organico , le materie dei ***poteri speciali*** che lo stesso può esercitare, anche al fine di aderire alle indicazioni e alle censure sollevate in sede europea, per salvaguardare gli assetti proprietari delle società operanti in settori reputati strategici e di interesse nazionale.

Per ***poteri speciali***, si intendono, tra gli altri, la facoltà di dettare specifiche condizioni all'acquisito di partecipazioni, di porre il veto all'adozione di determinate delibere societarie e di opporsi all'acquisto di partecipazioni. L'obiettivo del provvedimento è di rendere compatibile con il diritto europeo la disciplina nazionale dei poteri speciali del Governo, che si ricollega agli istituti della "*golden share*" e "*action spécifique*" – previsti rispettivamente nell'ordinamento inglese e francese - e che in passato era già stata oggetto di censure sollevate dalla Commissione europea e di una pronuncia di condanna da parte della Corte di giustizia UE.

Per mezzo del decreto-legge sono stati ridefiniti inoltre, anche mediante il rinvio ad atti di normazione secondaria (DPCM), l'ambito oggettivo e soggettivo, la tipologia, le condizioni e le procedure di esercizio da parte dello Stato (in particolare, del Governo) dei suddetti poteri speciali. Si tratta, in particolare, di poteri esercitabili nei settori della difesa e della sicurezza nazionale, nonché di taluni ambiti di attività definiti di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni.

Per definire i criteri di compatibilità comunitaria della disciplina dei poteri speciali, la Commissione europea ha adottato una apposita Comunicazione, con la quale ha affermato che l'esercizio di tali poteri deve comunque essere attuato senza discriminazioni ed è ammesso se si fonda su "criteri obiettivi, stabili e resi pubblici" e se è giustificato da "motivi imperiosi di interesse generale". Riguardo agli specifici settori di intervento, la Commissione ha ammesso un regime particolare per gli investitori di un altro Stato membro qualora esso sia giustificato da motivi di ordine pubblico, di pubblica sicurezza e di sanità pubblica purché, conformemente alla giurisprudenza della Corte di giustizia, sia esclusa qualsiasi interpretazione che poggi su considerazioni di ordine economico.

Nel settore fiscale e in quello della vigilanza prudenziale sulle istituzioni finanziarie, o con riguardo ai movimenti di capitali, le deroghe ammesse non devono costituire un mezzo di discriminazione arbitraria, né una restrizione dissimulata al libero movimento dei capitali. In ogni caso, secondo quanto indicato dalla Commissione, la definizione dei poteri speciali deve rispettare il principio di proporzionalità, vale a dire deve attribuire allo Stato solo i poteri strettamente necessari per il conseguimento dell'obiettivo perseguito. Gli indirizzi contenuti nella predetta Comunicazione hanno costituito la base per l'avvio da parte della Commissione delle procedure di infrazione nei confronti delle disposizioni del decreto-legge n. 332/1994, recanti la disciplina generale dei poteri speciali. Procedure di infrazione in materia di golden share hanno riguardato anche il Portogallo, il Regno Unito, la Francia, il Belgio, la Spagna e la Germania.

La principale differenza con la normativa precedente si rinviene nell'ambito operativo della nuova disciplina (articolo 1), che consente l'esercizio dei poteri speciali rispetto a tutte le società, pubbliche o private, che svolgono attività considerate di rilevanza strategica, e non più soltanto rispetto alle società privatizzate o in mano pubblica. Per effetto delle norme in commento, alla disciplina secondaria (decreti del Presidente del Consiglio dei Ministri) sono affidate le seguenti funzioni:

- individuazione di attività di rilevanza strategica per il sistema di difesa e sicurezza nazionale in rapporto alle quali potranno essere attivati i poteri speciali;
- individuazione della tipologia di atti o operazioni infragruppo esclusi dall'ambito operativo della nuova disciplina;
- concreto esercizio dei poteri speciali;
- individuazione di ulteriori disposizioni attuative.

Le norme fissano puntualmente il requisito per l'esercizio dei poteri speciali nei comparti della sicurezza e della difesa: la sussistenza di una minaccia di grave pregiudizio per gli interessi essenziali della difesa e della sicurezza nazionale. L'esecutivo può imporre specifiche condizioni all'acquisto di partecipazioni in imprese strategiche nel settore della difesa e della sicurezza, porre il veto all'adozione di delibere relative ad operazioni straordinarie o di particolare rilevanza, ivi incluse le modifiche di clausole statutarie eventualmente adottate in materia di limiti al diritto di voto o al possesso azionario e opporsi all'acquisto di partecipazioni, ove l'acquirente arrivi a detenere un livello della partecipazione al capitale in grado di compromettere gli interessi della difesa e della sicurezza nazionale.

Con il D.P.C.M. n° 253 del 30 novembre 2012, sono state individuate le attività di rilevanza strategica per il sistema di difesa e sicurezza nazionale al fine dell'esercizio dei poteri speciali e gli atti/operazioni infragruppo esclusi dall'ambito operativo della nuova disciplina. Con D.P.C.M. 2 ottobre 2013, n. 129 è stata prevista una modifica al citato D.P.C.M. 30 novembre 2012, n. 253, per far rientrare, ai fini dell'esercizio dei poteri speciali di cui all'articolo 1 del D.L. n. 21 del 2012, negli attivi di rilevanza strategica nel settore delle comunicazioni le reti e gli impianti utilizzati per la fornitura dell'accesso agli utenti finali dei servizi rientranti negli obblighi del servizio universale e dei servizi a banda larga e ultra larga. Tale modifica sembrava consentire l'applicazione anche a tali settori delle norme - più stringenti - previste per i comparti della difesa e della sicurezza nazionale. I due D.P.C.M. sono stati abrogati dal D.P.R. n. 108 del 2014 (si veda oltre).

Il D.P.C.M. n° 35 del 20 marzo 2014, n. 35 ha invece individuato le procedure per l'attivazione dei poteri speciali nei settori della difesa e della sicurezza nazionale.

Con il D.P.R. n° 108 del 6 giugno 2014, è stato adottato il Regolamento per l'individuazione delle attività di rilevanza strategica per il sistema di difesa e sicurezza nazionale. Si è provveduto, pertanto, a riunire in un unico regolamento le norme che individuano le attività di rilevanza strategica per il sistema di difesa e sicurezza nazionale, ivi incluse le attività strategiche chiave, di competenza sia del Ministero dell'interno, sia del Ministero della difesa, procedendo contestualmente all'abrogazione del citato D.P.C.M. n. 253 del 2012, come modificato dal D.P.C.M. n. 129 del 2013.

I poteri speciali nei comparti energia, trasporti e comunicazioni

Con disposizioni simili a quelle previste per il comparto sicurezza e difesa (articolo 2 del decreto-legge n. 21 del 2012), alla disciplina secondaria - attraverso regolamenti (anziché DPCM) da adottare previo parere delle Commissioni parlamentari competenti - sono affidate le seguenti funzioni:

- individuazione degli asset strategici nel settore dell'energia, dei trasporti e delle comunicazioni;
- esercizio dei poteri speciali;
- individuazione di ulteriori disposizioni attuative della nuova disciplina.

I poteri speciali esercitabili nel settore dell'energia, dei trasporti e delle comunicazioni consistono nella possibilità di far valere il veto dell'esecutivo alle delibere, agli atti e alle operazioni concernenti asset strategici, in presenza dei requisiti richiesti dalla legge, ovvero imporvi specifiche condizioni; di porre condizioni all'efficacia dell'acquisto di partecipazioni da parte di soggetti esterni all'UE in società che detengono attivi "strategici" e, in casi eccezionali, opporsi all'acquisto stesso. Le norme, in rapporto alle tipologie di poteri esercitabili e alle loro modalità di esercizio, ripropongono – con alcune differenze - la disciplina prevista dall'articolo 1 in relazione alle società operanti nel comparto difesa e sicurezza, secondo quanto segnalato di seguito.

Gli obblighi di notifica sono estesi alle delibere, atti o operazioni aventi ad oggetto il mutamento dell'oggetto sociale, lo scioglimento della società, la modifica di clausole statutarie riguardanti l'introduzione di limiti al diritto di voto o al possesso azionario. Il veto alle delibere, atti o operazioni può essere espresso qualora essi diano luogo a una situazione eccezionale, non disciplinata dalla normativa – nazionale ed europea - di

settore, di minaccia di grave pregiudizio per gli interessi pubblici relativi alla sicurezza e al funzionamento delle reti e degli impianti e alla continuità degli approvvigionamenti, ivi compresi le reti e gli impianti necessari ad assicurare l'approvvigionamento minimo e l'operatività dei servizi pubblici essenziali. Nel computo della partecipazione rilevante ai fini dell'acquisto si tiene conto della partecipazione detenuta da terzi con cui l'acquirente ha stipulato patti parasociali. Anche per le violazioni di cui al presente articolo è prevista la sanzione della nullità degli atti.

Sui regolamenti di attuazione è previsto un parere rinforzato del Parlamento: qualora i pareri espressi dalle Commissioni parlamentari competenti rechino identico contenuto, il Governo, ove non intenda conformarvisi, trasmette nuovamente alle Camere lo schema di regolamento, indicandone le ragioni in un'apposita relazione. I pareri definitivi delle Commissioni competenti sono espressi entro il termine di venti giorni dalla data di trasmissione. Decorso tale termine, il regolamento può essere comunque adottato.

I due regolamenti sono stati pubblicati nella Gazzetta Ufficiale del 6 giugno 2014 e sono entrati in vigore il 7 giugno 2014. Si tratta del D.P.R. 25 marzo 2014, n. 85 contenente il "Regolamento per l'individuazione degli attivi di rilevanza strategica" e del D.P.R. 25 marzo 2014, n. 86 contenente il "Regolamento per l'individuazione delle procedure per l'attivazione dei poteri speciali".

Le modifiche apportate dal decreto-legge n. 148 del 2017

Sulla disciplina del 2012 il legislatore è successivamente intervenuto (articolo 14 del decreto-legge n. 148 del 2016), in particolare:

1. prevedendo una generale sanzione amministrativa pecuniaria ove siano violati gli obblighi di notifica, funzionali all'esercizio dei poteri speciali da parte del Governo nel comparto della difesa e della sicurezza nazionale;
2. estendendo l'esercizio dei poteri speciali applicabili nei settori dell'energia, dei trasporti e delle comunicazioni, al settore della cd. alta intensità tecnologica;
3. individuando un criterio specifico cui il Governo deve attenersi nell'esercizio dei poteri speciali, con riferimento a quelle operazioni di acquisto da parte di soggetti extra UE di società che detengono attivi strategici nel settore energetico, dei trasporti e delle comunicazioni, ove l'acquisto di partecipazioni determini l'insediamento stabile dell'acquirente. In tali ipotesi il Governo deve valutare, oltre alla minaccia di grave pregiudizio agli interessi pubblici relativi alla sicurezza e al funzionamento delle reti e degli impianti e alla continuità degli approvvigionamenti, anche il pericolo per la sicurezza o per l'ordine pubblico;
4. chiarendo che alle sanzioni amministrative pecuniarie previste in materia di poteri speciali si applicano le disposizioni generali in materia di sanzioni amministrative di cui alla legge n. 689 del 1981, salva la possibilità di pagamento in misura ridotta.

Le norme così introdotte si applicano solo alle procedure avviate in data successiva al 16 ottobre 2017.

Altri poteri speciali

In via generale occorre ricordare che, oltre alla disciplina della golden share, altri interventi normativi hanno perseguito - con diverse modalità – scopi analoghi di tutela delle società operanti in settori giudicati strategici per l'economia nazionale.

In particolare, ulteriori diritti speciali in capo all'azionista pubblico sono stati previsti nella disciplina codicistica delle società, nonché, successivamente, nella legge 23 dicembre 2005, n. 266 (legge finanziaria 2006), che ha introdotto nell'ordinamento italiano la cd. poison pill (pillola avvelenata) che consente, in caso di offerta pubblica di acquisto ostile riguardante società partecipate dalla mano pubblica, di deliberare un aumento di capitale, grazie al quale l'azionista pubblico potrebbe accrescere la propria quota di

partecipazione vanificando il tentativo di scalata non concordata. Nella medesima logica di salvaguardia delle società d'interesse nazionale, s'innesta, da ultimo, l'articolo 7 del decreto-legge n. 34 del 2011, che ha autorizzato la Cassa Depositi e Prestiti ad assumere partecipazioni in società di rilevante interesse nazionale, in termini di strategicità del settore di operatività, di livelli occupazionali, di entità di fatturato ovvero di ricadute per il sistema economico-produttivo del Paese. In particolare, sono state definite "di rilevante interesse nazionale" le società di capitali operanti nei settori della difesa, della sicurezza, delle infrastrutture, dei trasporti, delle comunicazioni, dell'energia, delle assicurazioni e dell'intermediazione finanziaria, della ricerca e dell'innovazione ad alto contenuto tecnologico e dei pubblici servizi.

Ed è proprio in ambito telecomunicazioni che il sistema del golden power ha acquisito, di recente, nuova notorietà, in occasione dell'applicazione della disciplina ad opera del neocostituito governo Conte II sulle reti del 5G. Dal 2012 ad oggi, la disciplina riguardante le modalità di individuazione delle aree d'intervento, le modalità d'azione del consiglio dei Ministri e le conseguenze delle sue mosse ha conosciuto uno sviluppo importante col Dpcm 6 agosto 2014, messo in campo dal governo Renzi, che ha garantito una più corposa definizione del perimetro di pertinenza della misura.

Nello 2017 il governo Gentiloni utilizzò il golden power per fermare l'azione di Vincent Bolloré e del suo colosso francese Vivendi nel campo delle tlc nazionali italiane, che avevano portato l'arrembante finanziere transalpino a cercare di mettere le mani su Tim. Nel 2019 abbiamo avuto il già citato intervento del governo Conte II, attraverso il suo primo atto ufficiale, sul terreno del 5G attraverso l'esercizio del golden power per condizionare e supervisionare le relazioni di Linkem, Vodafone, Tim, Wind Tre e Fastweb con le cinesi Huawei e Zte.

Il ruolo chiave dell'intelligence

Il golden power è diventato, come scrive l'Agi, "il pulsante di stop" nelle mani del governo, ed è uno strumento che acquisirà sempre maggior valore mano a mano che aumenterà l'interesse strategico per il sistema-Paese Italia, principalmente ad opera delle aziende di Paesi extra-Ue e extra-Nato come, ad esempio, la Cina.
Risulta vitale per l'Italia, tutelarsi ed evitare di essere schiacciati tra l'incudine della silenziosa infiltrazione del Dragone, ed il martello dell'inevitabile rappresaglia economica e politica degli alleati, Usa innanzitutto.

Il golden power è dunque da vedere non come un limite o condizionamento all'attività di impresa, ma come un vero e proprio strumento di garanzia dell'economia nazionale. Su questo vegliano come guardiani, i servizi di sicurezza e intelligence, autori di un'ampia campagna di sensibilizzazione sul tema, culminata in una recente pubblicazione del Dis, il Dipartimento per le informazioni di sicurezza. "Tutto il supporto dei servizi segreti all'azione del governo non è teso a convincerlo nelle scelte e neanche orientarlo" scrive al suo interno Alessandro Pansa, ex capo della polizia e del Dis, "ma a suggerire percorsi da intraprendere per rendere quanto più informato e consapevole il decisore politico che opererà poi le sue scelte che sottendono a strategie di cui l'intelligenza è destinataria e non originatrice".

La competizione internazionale si fa sempre più decisa e complessa, e al governo servono strumenti di tutela che sappiano imporre, nei momenti cruciali, il ruolo della politica su quello dei mercati. E il golden power va proprio in questa direzione.

Golden Power rafforzato per 5G e Cloud. Tutte le modifiche alle norme sui poteri speciali introdotte con il decreto Ucraina a marzo 2022

Golden Power è così rafforzato per quanto riguarda 5G e Cloud, con quest'ultimo che per la prima volta assurge a infrastruttura critica per la sicurezza nazionale. Lo prevede il "Decreto Ucraina" (Misure urgenti per contrastare gli effetti economici e umanitari della crisi ucraina) varato dal governo lo scorso venerdì 18 marzo (si veda qui il comunicato stampa)

Nel dettaglio, spiega la nota della Presidenza del Consiglio dei Ministri, "si interviene per rafforzare la disciplina del controllo degli investimenti stranieri in Italia, finalizzata all'esercizio dei poteri speciali spettanti al Governo (c.d. "golden power"), alla luce dell'accresciuta strategicità di alcuni settori e della necessità di potenziare le strutture amministrative coinvolte".

- Tra le misure introdotte, si segnalano le seguenti:nei settori della difesa e della sicurezza nazionale, le operazioni oggetto di notifica comprenderanno anche quelle che hanno per effetto modifiche alla titolarità o alla disponibilità degli attivi, similmente a quanto avviene oggi per gli altri settori;
- è introdotta, per l'impresa acquirente e per l'impresa target, la notifica congiunta dell'operazione, in modo da evitare una notifica da parte dell'impresa acquirente e una notifica successiva da parte dell'impresa target una volta rinnovati gli organi sociali;
- sono stabilizzate, quanto al termine di efficacia che verrebbe meno il 31 dicembre 2022, alcune previsioni relative sia all'obbligo di notifica delle acquisizioni di minoranza da parte di operatori extra-UE, sia all'obbligo di notifica delle acquisizioni di controllo da parte di operatori intra-UE;
- è rivista la disciplina dei poteri speciali inerenti le reti di telecomunicazione elettronica a banda larga con tecnologica 5G e cloud (art. 28 della bozza di Decreto)
- saranno individuate misure di semplificazione delle modalità di notifica delle operazioni, dei termini e delle procedure relativi all'istruttoria, senza che sia necessaria la delibera del Consiglio dei ministri, per la definizione dei procedimenti in caso di mancato esercizio dei poteri speciali;

saranno altresì individuate le modalità di presentazione di una pre-notifica delle operazioni al fine di ricevere una preliminare valutazione circa l'effettiva applicabilità della disciplina in materia di golden power e l'autorizzabilità dell'operazione.

Con l'art. 29 della bozza di Decreto è stato inoltre previsto un rafforzamento della disciplina sulla cybersicurezza e in particolare si prevede la sostituzione di tecnologie russe. Al fine di prevenire pregiudizi alla sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, queste procedono tempestivamente alla diversificazione dei prodotti in uso, anche mediante procedure negoziate. Le procedure di acquisto riguarderanno determinate categorie di prodotti e servizi sensibili quali applicativi antivirus, antimalware, endpoint detection and response (EDR) e web application firewall (WAF).

Il Decreto Liquidità varato in piena prima fase della pandemia (si veda altro articolo di BeBeez) aveva ampliato temporaneamente in maniera orizzontale i settori oggetto del controllo governativo, ma anche in maniera verticale, includendo anche aziende non quotate e di qualunque dimensione, sempre all'interno di un elenco preciso di settori classificati come strategici, ha poi ampliato il perimetro del golden power, estendendo i poteri di veto e interdizione del governo a tutti i settori strategici individuati nell'art. 4 comma 1 del Regolamento UE 2019/452, cioè quelli: assicurativo, del credito, della finanza, dell'acqua, della salute, della cybersicurezza, delle nano- e bio-tecnologie, delle comunicazioni e dei media, del trattamento o archiviazione di dati, delle infrastrutture aerospaziali, di difesa, elettorali o finanziarie, delle strutture sensibili. degli investimenti in terreni e immobili fondamentali per l'utilizzo di tali infrastrutture. Non solo. In

sede di conversione in legge, nel Decreto Liquidità era stato specificato che devono intendersi compresi nel settore finanziario, i settori creditizio e assicurativo e nel settore sanitario, la produzione, l'importazione e la distribuzione all'ingrosso di dispositivi medicali, medico-chirurgici e di protezione individuale.

I concetti contenuti nel Decreto Liquidità erano stati poi ulteriormente precisati nel DCPM del 30 dicembre 2020 . Mentre tutte le misure temporanee in questione sono state nel frattempo estese sino a fine 2022.

Come la gestione della pandemia, anche la sicurezza nazionale deve uscire da una logica emergenziale. La riorganizzazione della struttura di Palazzo Chigi preposta al golden power che persegue proprio questo obiettivo. Secondo l'agenzia americana Reuters,e fonti del governo a breve il Governo emenera un Dpcm a firma del Premier Mario Draghi per dar via ad una specifica Direzione generale per la vigilanza delle imprese e degli asset strategici.

La nuova struttura avrà due funzioni. Da una parte l'esame delle notifiche, dall'altra l'attività di analisi strategica dei movimenti di mercato che hanno un potenziale impatto sulla sicurezza nazionale. L'idea parte da lontano e più precisamente dal 2018.

Negli ultimi anni infatti le notifiche delle aziende al governo hanno visto un'impennata. Il record nel 2021 con 496 segnalazioni, rispetto alle 341 dell'anno precedente. Un'enorme mole di lavoro per i tecnici di Palazzo Chigi. Dovuta anche e soprattutto all'allargamento del golden power alla rete 5G, inserito nel "decreto Brexit" del marzo 2019 (art. 1-bis) e recepito dal "decreto cyber" (105/2019) con cui si è dato vita al perimetro cyber nell'autunno dello stesso anno. Lo scudo a tutela degli asset strategici è stato poi ampliato durante il primo anno di pandemia, in risposta alla direttiva Ue sugli investimenti esteri e di nuovo, due settimane fa, dal governo Draghi nel "Decreto Ucraina" per il 5G e il Cloud.

Di qui l'esigenza di una riorganizzazione della struttura. La ratio è evitare un'analisi caso per caso e unire al controllo delle notifiche una strategia industriale coerente, con un confronto preventivo con le imprese. Per questo, tra le altre novità, sarà introdotto l'istituto della "pre-notifica". Le aziende dovranno cioè avvisare il governo prima che una modifica dell'assetto societario o un'operazione di M&A rientrante nei settori coperti dal golden power vada in porto.

Un sistema che può aiutare ad alleggerire le procedure evitando un intervento solo ex-post di Palazzo Chigi che – è il caso di un'azienda quotata in borsa – può avere dure conseguenze. Ma avrà anche un doppio effetto benefico. Da una parte ridurrà la mole spropositata di notifiche inutili che ogni anno le aziende prese dall'incertezza inviano al governo.

Dall'altra diminuiranno i casi in cui la notifica, dovuta, non viene inviata. È successo nella vicenda Alpi Aviation, l'azienda italiana produttrice di droni che non ha notificato alla Presidenza del Consiglio la vendita, avvenuta nel 2018, del 75% delle quote a una società di Hong Kong controllata a sua volta da due gruppi statuali cinesi, annullata poi con un decreto del governo.

Il modello di riferimento guarda oltreoceano al triage, il sistema seguito dal comitato di controllo degli investimenti esteri americano, il Cfius, che prevede una continua interlocuzione del governo federale con le aziende e dà alle autorità un'immagine più chiara di quali operazioni siano state notificate e quali no. "L'istituzione di una Direzione generale va nella giusta direzione perché permette di affrontare la tutela degli asset sensibili con una visione più strategica di quanto non si faccia ora", spiega a Formiche.net Giacomo Vigna, già componente del gruppo di coordinamento a Palazzo Chigi e consulente economico dell'allora Sottosegretario di Stato Giorgetti. "Questo può accadere se la nascente DG saprà coordinarsi nel merito degli aspetti riguardanti la politica industriale, energetica ed economica in senso molto ampio. Il coordinamento dovrà avvenire sia con le istituzioni ad oggi coinvolte che con le autorità amministrative di settore che la legge già prevede possano e debbano cooperare con il Governo perché il Golden power funzioni".

Con la nuova direzione generale si completa un lungo percorso di riassetto e rafforzamento dell'apparato preposto alla tutela degli asset strategici. Tra le altre facoltà, grazie a una modifica alla normativa del giugno del 2019, i tecnici di Chigi possono oggi chiedere informazioni ad agenzie o enti pubblici senza che possa loro essere opposto il segreto istruttorio.

Rimangono tuttavia dubbi da chiarire sull'ultimo intervento del governo per rafforzare i poteri speciali. Come la previsione dell'obbligo in capo alle aziende di presentare ai tecnici del governo un "piano annuale degli acquisti". Un passaggio controverso perché, fanno notare gli addetti ai lavori, a differenza delle Pa, che dispongono di un budget annuale predeterminato, le aziende si trovano spesso e volentieri a dover cambiare il piano acquisti per esigenze di mercato. Vale tanto più per il settore Ict – ad esempio i fornitori e operatori della rete 5G – che fanno i conti con tecnologie mutevoli e devono stare al passo con l'innovazione.

Qui di seguito si segnalano i due articoli più rilevanti, il 27 e 28.

ART. 27

(Ridefinizione dei poteri speciali in materia di comunicazione elettronica a banda larga basati sulla tecnologia 5G e cloud)

1. L'articolo 1-bis del decreto-legge 15 marzo 2012, n. 21, convertito, con modificazioni, dalla legge 11 maggio 2012, n. 56, è sostituito dal seguente:

"Art. 1-bis

Poteri speciali inerenti le reti di telecomunicazione elettronica a banda larga con tecnologia 5G, basati sulla tecnologia cloud e altri attivi
1. Ai fini dell'esercizio dei poteri speciali di cui al presente articolo, costituiscono attività di rilevanza strategica per il sistema di difesa e sicurezza nazionale i servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G. Ulteriori beni, rapporti, attività e tecnologie rilevanti ai fini della sicurezza cibernetica, ivi inclusi quelli relativi alla tecnologia cloud, possono essere individuati con uno o più decreti del Presidente del Consiglio dei ministri, di concerto con il Ministro per lo sviluppo economico, il Ministro dell'interno, il Ministro della difesa, il Ministro per gli affari esteri e la cooperazione internazionale, il Ministro per l'innovazione tecnologica e la transizione digitale, ove nominato, e con gli altri Ministri competenti per settore, e sentita l'Agenzia per la cybersicurezza nazionale, anche in deroga all'articolo 17 della legge 23 agosto 1988, n. 400, previo parere delle Commissioni parlamentari competenti, che è reso entro trenta giorni, decorsi i quali i decreti sono adottati anche in mancanza di parere.

2. Fermi gli obblighi previsti ai sensi del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, le imprese che, anche attraverso contratti o accordi, intendano acquisire, a qualsiasi titolo, beni o servizi relativi alla progettazione, alla realizzazione, alla manutenzione e alla gestione delle attività di cui al comma 1, ovvero componenti ad alta intensità tecnologica funzionali alla predetta realizzazione o gestione, notificano, prima di procedere alla predetta acquisizione, alla Presidenza del Consiglio dei ministri un piano annuale nel quale sono contenuti: il settore interessato dalla notifica; dettagliati dati identificativi del soggetto notificante; il programma di acquisti; dettagliati dati identificativi dei relativi, anche potenziali, fornitori; dettagliata descrizione, comprensiva delle specifiche tecniche, dei beni, dei servizi e delle componenti ad alta intensità tecnologica funzionali alla progettazione, alla realizzazione, alla manutenzione e alla gestione delle attività di cui al comma 1; un'informativa completa sui contratti in corso e sulle prospettive di sviluppo della rete 5G, ovvero degli ulteriori sistemi e attivi di cui al comma 1; ogni ulteriore informazione funzionale a fornire un dettagliato quadro delle modalità di sviluppo dei sistemi di digitalizzazione del notificante, nonché dell'esatto adempimento alle condizioni e alle prescrizioni imposte a seguito di precedenti notifiche; un'informativa completa relativa alle

eventuali comunicazioni effettuate ai sensi dell'articolo 1, comma 6, lettera a), del decreto-legge 21 settembre 2019, n. 105, ai fini dello svolgimento delle verifiche di sicurezza da parte del Centro di valutazione e certificazione nazionale (CVCN), inclusiva dell'esito della valutazione, ove disponibile, e delle relative prescrizioni, qualora imposte. Con uno dei decreti di cui al comma 1, ovvero con diverso decreto adottato con il medesimo procedimento, possono altresì essere individuati ulteriori contenuti del piano annuale, eventuali ulteriori criteri e modalità con cui procedere alla notifica del medesimo piano, oltre ad eventuali tipologie di attività escluse dall'obbligo di notifica, anche in considerazione delle ridotte dimensioni dell'operazione.

3. La notifica di cui di cui al comma 2 è trasmessa annualmente, prima di procedere all'attuazione del piano, salva la possibilità di aggiornarlo in corso di anno, con cadenza quadrimestrale. Entro trenta giorni dalla notifica, con decreto del Presidente del Consiglio dei ministri, adottato su conforme delibera del Consiglio dei ministri, è approvato il piano annuale di cui al comma 2, previa eventuale imposizione di prescrizioni o condizioni, ovvero ne è negata l'approvazione con l'esercizio del potere di veto. Salvo diversa previsione nel decreto di approvazione del piano, rimane ferma l'efficacia dei decreti del Presidente del Consiglio dei ministri già adottati alla data di entrata in vigore del presente articolo. Se è necessario svolgere approfondimenti riguardanti aspetti tecnici anche relativi alla valutazione di possibili fattori di vulnerabilità, che potrebbero compromettere l'integrità e la sicurezza delle reti, dei dati che vi transitano o dei sistemi, il termine di trenta giorni previsto dal presente comma può essere prorogato fino a venti giorni, prorogabili ulteriormente di venti giorni, per una sola volta, in casi di particolare complessità. Se nel corso dell'istruttoria si rende necessario richiedere informazioni al notificante, tale termine è sospeso, per una sola volta, fino al ricevimento delle informazioni richieste, che sono rese entro il termine di dieci giorni. Se si rende necessario formulare richieste istruttorie a soggetti terzi, il predetto termine di trenta giorni è sospeso, per una sola volta, fino al ricevimento delle informazioni richieste, che sono rese entro il termine di venti giorni. Le richieste di informazioni e le richieste istruttorie a soggetti terzi successive alla prima non sospendono i termini. In caso di incompletezza della notifica, il termine di trenta giorni previsto dal presente comma decorre dal ricevimento delle informazioni o degli elementi che la integrano. Decorsi i predetti termini, il piano si intende approvato.

4. I poteri speciali sono esercitati nella forma dell'imposizione di specifiche prescrizioni o condizioni ogniqualvolta ciò sia sufficiente ad assicurare la tutela degli interessi essenziali della difesa e della sicurezza nazionale. A tal fine, sono oggetto di valutazione anche gli elementi indicanti la presenza di fattori di vulnerabilità che potrebbero compromettere l'integrità e la sicurezza delle reti e dei dati che vi transitano, compresi quelli individuati sulla base dei principi e delle linee guida elaborati a livello internazionale e dall'Unione europea. Se le prescrizioni o condizioni non risultano sufficienti ad assicurare la tutela dei citati interessi, il Governo, tenendo conto dei contenuti del piano notificato, dell'obsolescenza, del costo e dei tempi di sostituzione degli apparati e dell'esigenza di non rallentare lo sviluppo della tecnologia 5G o di altre tecnologie nel Paese, nel rispetto dei principi di proporzionalità e adeguatezza, approva, in tutto o in parte, il piano per un periodo temporale, anche limitato, indicando un termine per l'eventuale sostituzione di determinati beni o servizi ovvero non approva il piano esercitando il potere di veto.
5. Salvo quanto previsto dal presente comma, se il soggetto notificante inizia l'esecuzione di contratti o accordi, successivi all'entrata in vigore del presente articolo, compresi nella notifica prima che sia decorso il termine per l'approvazione del piano, il Governo può ingiungere all'impresa, stabilendo il relativo termine, di ripristinare a proprie spese la situazione anteriore all'esecuzione del predetto contratto o accordo. Salvo che il fatto costituisca reato, chiunque non osserva gli obblighi di notifica di cui al presente articolo ovvero le disposizioni contenute nel provvedimento di esercizio dei poteri speciali è soggetto alla sanzione amministrativa pecuniaria fino al tre per cento del fatturato del soggetto tenuto alla notifica. I contratti eventualmente stipulati in violazione delle prescrizioni o delle condizioni contenute nel provvedimento di esercizio dei poteri speciali sono nulli. Il Governo può altresì ingiungere all'impresa, stabilendo il relativo termine, di ripristinare a proprie spese la situazione anteriore alla violazione, applicando una sanzione amministrativa pecuniaria sino a un dodicesimo di quella prevista al periodo precedente per ogni mese di ritardo nell'adempimento,

commisurata al ritardo. Analoga sanzione può essere applicata per il ritardo nell'adempimento dell'ingiunzione di cui al primo periodo del presente comma. Nei casi di violazione degli obblighi di notifica di cui al presente articolo, anche in assenza della notifica, la Presidenza del Consiglio dei ministri può avviare d'ufficio il procedimento ai fini dell'eventuale esercizio dei poteri speciali. A tale scopo, trovano applicazione i termini e le norme procedurali previsti dal presente articolo. Il termine di trenta giorni di cui al comma 3 decorre dalla conclusione del procedimento di accertamento della violazione dell'obbligo di notifica.

6. Per l'esercizio dei poteri speciali di cui al presente articolo il gruppo di coordinamento per l'esercizio dei poteri speciali è composto dai rappresentanti della Presidenza del Consiglio dei ministri, del Ministero dello sviluppo economico, del Ministero dell'economia e delle finanze, del Ministero dell'interno, del Ministero della difesa, del Ministero per gli affari esteri e la cooperazione internazionale, dal Ministro per l'innovazione tecnologica e la transizione digitale, ove previsto, nonché dai rappresentanti dell'Agenzia per la cybersicurezza nazionale. Il gruppo di coordinamento si avvale anche del Centro di valutazione e certificazione nazionale (CVCN), istituito presso l'Agenzia per la cybersicurezza nazionale, e delle articolazioni tecniche dei Ministeri dell'interno e della difesa, per le valutazioni tecniche della documentazione relativa al piano annuale di cui al comma 2, e ai suoi eventuali aggiornamenti, propedeutiche all'esercizio dei poteri speciali e relative ai beni e alle componenti ad alta intensità tecnologica funzionali alla progettazione, alla realizzazione, alla manutenzione e alla gestione delle attività di cui al comma 1 nonché ad altri possibili fattori di vulnerabilità che potrebbero compromettere l'integrità e la sicurezza delle reti, dei dati che vi transitano o dei sistemi.

7. Le attività di monitoraggio, tese alla verifica dell'osservanza delle prescrizioni e delle condizioni impartite con il provvedimento di esercizio dei poteri speciali, alla analisi della relativa adeguatezza e alla verifica dell'adozione di adeguate misure, anche tecnologiche, attuative delle medesime prescrizioni o condizioni sono svolte da un comitato composto da uno o più rappresentanti della Presidenza del Consiglio dei ministri, del Ministero dello sviluppo economico, del Ministero per l'innovazione tecnologica e la transizione digitale, o, se non nominato della struttura della Presidenza del Consiglio dei ministri competente per l'innovazione tecnologica e la digitalizzazione, dell'Agenzia per la cybersicurezza nazionale. Per le attività di monitoraggio, il comitato si avvale anche del Centro di valutazione e certificazione nazionale (CVCN), istituito presso l'Agenzia per la cybersicurezza nazionale e delle articolazioni tecniche dei Ministeri dell'interno e della difesa. Ai lavori del comitato di monitoraggio possono essere chiamati a partecipare altri rappresentanti dei Ministeri di cui al comma 6. Al fine del concreto esercizio delle attività di monitoraggio il soggetto interessato comunica con la periodicità indicata con il provvedimento di esercizio dei poteri speciali, ogni attività esecutiva posta in essere, ivi inclusa la stipulazione dei contratti ad essa riferiti, fornendo ogni opportuno dettaglio tecnico ed evidenziando le ragioni idonee ad assicurare la conformità della medesima al piano approvato ai sensi del comma 3. Il soggetto interessato trasmette altresì, una relazione periodica semestrale sulle attività in corso. È fatta salva la possibilità per il comitato di monitoraggio di disporre ispezioni e verifiche tecniche, anche con le modalità di cui all'articolo 2-bis, relativamente ai beni e alle componenti ad alta intensità tecnologica funzionali alla progettazione, alla realizzazione, alla manutenzione e alla gestione delle attività di cui al comma 1 nonché ad altri possibili fattori di vulnerabilità che potrebbero compromettere l'integrità e la sicurezza delle reti, dei dati che vi transitano o dei sistemi, oggetto del provvedimento di esercizio dei poteri speciali. L'inosservanza delle prescrizioni o delle condizioni contenute nel provvedimento di approvazione ovvero qualsiasi altra circostanza idonea a incidere sul provvedimento approvativo è segnalata al gruppo di coordinamento dell'esercizio dei poteri speciali di cui al comma 6, il quale può proporre al Consiglio dei ministri l'applicazione delle sanzioni previste dal comma 7, la revoca o la modifica del provvedimento autorizzativo e il divieto di esercizio delle attività funzionali alla progettazione, alla realizzazione, alla manutenzione e alla gestione delle attività di cui al comma 1.
8. Con decreto del Presidente del Consiglio dei ministri, sentito il Gruppo di coordinamento costituito ai sensi del comma 6 del presente articolo, anche in deroga all'articolo 17 della legge 23 agosto 1988, n. 400, possono essere individuate misure di semplificazione delle modalità di notifica, dei termini e

delle procedure relativi all'istruttoria ai fini dell'eventuale esercizio dei poteri di cui al presente articolo."

In sede di prima applicazione, il piano di cui al comma 2 dell'articolo 1-bis, del citato decreto- legge n. 21 del 2012, come modificato dal presente articolo, include altresì l'informativa completa sui contratti o sugli accordi relativi ai servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G già autorizzati. Ferma l'efficacia dei decreti del Presidente del Consiglio dei ministri già adottati ai sensi dell'articolo 1-bis del decreto legge n. 21 del 2012, i procedimenti in corso alla data di entrata in vigore del presente decreto sono dichiarati estinti dal predetto gruppo di coordinamento e il relativo esame è effettuato in sede di valutazione del piano annuale, fermo restando quanto previsto dai commi 3 e 5 dell'art. 1-bis del decreto legge n. 21 del 2012.

Dalla data di entrata in vigore del presente articolo è abrogato l'articolo 16, comma 10, del decreto-legge 14 giugno 2021 n. 82, convertito, con modificazioni, in legge 4 agosto 2021 n. 109.

CAPO II
Cybersicurezza delle reti, dei sistemi informativi e dei servizi informatici e degli approvvigionamenti

ART. 28

(Rafforzamento della disciplina cyber)

1. Al fine di prevenire pregiudizi alla sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, derivanti dal rischio che le aziende produttrici di prodotti e servizi tecnologici di sicurezza informatica legate alla Federazione Russa non siano in grado di fornire servizi e aggiornamenti ai propri prodotti appartenenti alle categorie individuate al comma 3, in conseguenza della crisi in Ucraina, le medesime amministrazioni procedono tempestivamente alla diversificazione dei prodotti in uso.
2. Le stazioni appaltanti, che procedono ai sensi del comma 1, provvedono all'acquisto di un ulteriore prodotto o servizio tecnologico di sicurezza informatica di cui al comma 3 e connessi servizi di supporto mediante gli strumenti di acquisto messi a disposizione dalle centrali di committenza, ovvero, laddove non sussistano o non siano comunque disponibili nell'ambito di tali strumenti, ai sensi dell'articolo 63, comma 1, del decreto legislativo 16 aprile 2016, n. 50. Si applicano le disposizioni di cui al comma 5, secondo, terzo e quarto periodo del medesimo articolo 63.
3. Le categorie di prodotti e servizi di cui al comma 1 sono indicate con circolare dell'Agenzia per la cybersicurezza nazionale, tra quelle volte ad assicurare le seguenti funzioni di sicurezza:
a) sicurezza dei dispositivi (endpoint security), ivi compresi applicativi antivirus, antimalware ed "endpoint detection and response" (EDR);
4. b) "web application firewall" (WAF);
Dall'attuazione dei commi 1 e 2 non derivano effetti che possano costituire presupposto per l'azione di responsabilità di cui all'articolo 1 della legge 14 gennaio 1994, n. 20.
5. Agli oneri derivanti dall'attuazione del presente articolo, pari ad euro _____, si provvede mediante corrispondente riduzione …….
6. Il Ministro dell'economia e delle finanze è autorizzato ad apportare, con propri decreti, le occorrenti variazioni di bilancio.
7. All'articolo 5, comma 1, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, dopo le parole "fattore di rischio o alla sua mitigazione," sono inserite le seguenti: "in deroga ad ogni disposizione vigente, nel rispetto dei principi generali dell'ordinamento giuridico e" e, in fine, sono aggiunti i seguenti periodi: "Laddove nei provvedimenti di cui al presente comma sia recata deroga alle leggi vigenti anche ai fini delle ulteriori necessarie misure correlate alla disattivazione o all'interruzione, gli stessi provvedimenti devono contenere l'indicazione delle principali norme a cui si intende derogare e tali deroghe devono

essere specificamente motivate. I provvedimenti di cui al presente comma non sono soggetti al controllo preventivo di legittimità di cui all'articolo 3 della legge 14 gennaio 1994, n. 20.".

5. Al fine di consentire il più rapido avvio delle attività strumentali alla tutela della sicurezza nazionale nello spazio cibernetico, all'articolo 12 del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, è aggiunto, in fine, il seguente comma: "8-bis. In relazione alle assunzioni a tempo determinato di cui al comma 2, lettera b), i relativi contratti per lo svolgimento delle funzioni volte alla tutela della sicurezza nazionale nello spazio cibernetico attribuite all'Agenzia stessa, possono prevedere una durata massima di 4 anni, rinnovabile per periodi non superiori ad ulteriori complessivi quattro anni. Delle assunzioni e dei rinnovi disposti ai sensi del presente comma è data comunicazione al COPASIR nell'ambito della relazione di cui all'articolo 14, comma 2.".

Infine si ricorda che lo scorso febbraio Il Comitato parlamentare per la Sicurezza della Repubblica (**Copasir**), nella sua Relazione annuale al Parlamento sull'attività svolta dal primo gennaio 2021 al 9 febbraio 2022, ha caldeggiato l'ipotesi che la normativa sul Golden Power possa essere estesa anche alla fase di due diligence, preliminare quindi al momento effettivo dell'acquisizione di una società italiana ritenuta strategica da parte di un investitore estero del costo e dei tempi di sostituzione degli apparati e dell'esigenza di non rallentare lo sviluppo della tecnologia 5G o di altre tecnologie nel Paese, nel rispetto dei principi di proporzionalità e adeguatezza, approva, in tutto o in parte, il piano per un periodo temporale, anche limitato, indicando un termine per l'eventuale sostituzione di determinati beni o servizi ovvero non approva il piano esercitando il potere di veto".

Si parla inoltre di "Rafforzamento della disciplina cyber" e si fa esplicita menzione delle "aziende produttrici di prodotti e servizi tecnologici di sicurezza informatica legate alla Federazione Russa" che "non siano in grado di fornire servizi e aggiornamenti ai propri prodotti appartenenti alle categorie individuate, in conseguenza della crisi in Ucraina". Il riferimento all'antivirus Kaspersky è chiaro, e si ordina alle amministrazioni che usano software russo di procedere "tempestivamente alla diversificazione dei prodotti in uso".

Nelle ultime settimane si sono intensificate le offensive, rivendicati dal collettivo filorusso Killnet, di attacchi hacker verso siti Istituzionali e non italiani.

I problemi più gravi riguardano la Polizia di Stato, il Ministero della Difesa, la Farnesina e il Csm. Aperta un'inchiesta dai Pm antiterrorismo di Roma. Per l'Autorità Delegata, il Sottosegretario Franco Gabrielli: "Dobbiamo prepararci per una escalation"

L'attacco hacker simultaneo ha preso di mira una cinquantina di indirizzi istituzionali italiani, la conferma dell'offensiva è arrivata anche dalle strutture di difesa del nostro Paese, a iniziare dall'ACN e dalla Polizia Postale, che sono impegnate a minimizzare la portata dei danni e a neutralizzare l'offensiva. Secondo quanto scritto dal gruppo di hacker l'attacco avrebbe riguardato siti come quello del Consiglio Superiore della Magistratura, del ministero degli esteri e dell'agenzia delle dogane.

Diventi quindi assolutamente prioritario anche per il Gruppo di Coordinamento per l'esercizio dei poteri speciali, (di cui all'articolo 3 del Dpcm 6/8/2014) del *Dipartimento per il Coordinamento Amministrativo Ufficio per la concertazione amministrativa e il monitoraggio*, rafforzare le verifiche nei confronti di quegli Operatori Economici esteri, ancorché sotto embargo, che procedono ad acquisizioni di aziende italiane o parte di esse, che detengono asset strategici non solo per la sicurezza nazionale ma anche per il semplice rischio di infiltrazioni nel sistema pubblico e privato della comunità nazionale.

Fonti: Presidenza del Consiglio dei Ministri; Ministero dello Sviluppo Economico; Dipartimento Politiche Europee; Knosso®; Formiche.Net